Supplementary Reference: 545, 552
File Name: 545sac_040500
Last Revised: 04/05/2000

AUTOMATED INFORMATION SYSTEM CERTIFICATION AND APPROVAL TO OPERATE

Consistent with ADS E545.5.1a **and E552.5.1a,** and Office of Management and Budget Circular A130, automated information systems that process or store classified national security information are required to be certified prior to processing or storing such information. In response to this requirement, the "ISSO for USAID" provides the following automated information system certification and approval to operate procedures for all systems used to process sensitive and classified national security information.

I**.** Certification

Certification is a technical evaluation of a system conducted as part of and in support of the approval to operate process. It establishes a level of data and information processing and storage that may take place using any or all components of an automated information system, and is based on USAID security policy promulgated in USAID ADS chapters 561, 545 **and 552**.

Certification has two component elements:

- A requirements analysis; and

- A facility security plan.

Both elements must be completed by cleared U.S. citizen personnel, within the requesting bureau, office, or mission, working under the supervision of a senior supervisory authority. Upon completion, the requirements analysis and facility security plan are to be forwarded to the "ISSO for USAID" for action within M/IRM.

A**.** Requirements Analysis

A requirements analysis identifies the need to process SBU or national security information. The format of the requirements analysis is at the discretion of the requesting entity; however, it must:

1. Justify a need for processing sensitive but unclassified **(**SBU**)** or classified national security information;

2. Identify the types of classified information or data that require

processing (e.g., cables, reports, spreadsheets, etc.);

3. Identify the highest classification level of information that needs to be processed (i.e., SBU, CONFIDENTIAL or SECRET);

4. Locate, on a facility blueprint-type drawing, the location of all system components, workstations, printers and other peripheral devices. If certification to process national security information is being requested, indicate the measured distance from each system component, workstation, and printer from communication devices (e.g., FAX machines, modems, telephones, etc.), public access areas and non-U.S. Government controlled space;

5. Provide the name, office symbol, business address, and office telephone number of the individual formally designated as the site Information systems security Officer (ISSO) responsible for the system; and

6. Identify the location of the nearest U.S. Government facility that processes classified national security information (e.g., U.S. Embassy, U.S. Consulate, Department of Defense installation, or neighboring USAID entity).

B**.** Facility Security Plan

A facility security plan contains specific security procedures for safeguarding a system and the data it processes. The format of the facility security plan is at the discretion of the requesting entity. However, it must include:

1. A configuration drawing of all system components, workstations, printers, modems, and other peripheral devices;

2. A description of the door locks used to control physical access to the system and its components, workstations, printers, modems, and other peripheral devices;

3. An identification, by type and location, of the security containers used to safeguard classified material and media produced as a result of classified processing operations;

4. A location specific procedure for destroying classified material and media;

5. A plan for application software and data backup as well as emergency actions;

6. A memorandum designating specific individuals responsibility for overall system management, system security (site ISSO and alternate), and local/regional U.S. security personnel. If certification to process national security information is being requested, all designees must have current security clearances and be U.S. citizens; and

7. In cases where certification to process national security information is being requested, a memorandum from the Regional Security Officer (RSO) or Office of Security (SEC) acknowledging the system and all of its components, workstations, cables, printers, modems and other peripheral devices are compliant with the prevailing red/black installation requirements (available from the "ISSO for USAID" and/or RSO).

II. Approval

Approval is the formal authorization for a system to process information at a specified level of sensitivity in an operational environment. It is based upon validation that a system is installed and operated in compliance with specified USAID security requirements (identified in USAID ADS, Security Guidance and Chapter**s** 545 **and 552**). All automated information system approvals shall be granted by the Director of M/IRM upon the recommendation of the "ISSO for USAID."

The "ISSO for USAID" is tasked with processing and evaluating all requests for automated information system certification and approval.

The approval process shall include the following procedures:

1. The requesting bureau, office or mission shall forward to the "ISSO for USAID" a requirements analysis and facility security plan (assistance in completing these documents is available upon request from M/IRM/IPA);

2. The "ISSO for USAID" shall conduct or direct the conduct of an evaluation of the requirements analysis and facility security plan;

3. The "ISSO for USAID" shall request SEC to verify that all required physical security controls are in-place and operating as designed;

4. The "ISSO for USAID" shall provide security awareness briefings for all personnel authorized to process classified national security information. If briefings are not feasible, the "ISSO for USAID" shall provide the site ISSO with training and awareness materials;

5. Upon completion of the aforementioned, the "ISSO for USAID" shall recommend to the Director of M/IRM approval or refusal of an automated information system to process SBU or classified national security information; and

6. The Director of M/IRM shall provide to the senior official of the requesting bureau, office or mission, a memorandum that formally grants a system approval to process SBU or national security classified information. If a system is refused approval to process a specific level of information, the reason for refusal shall be provided the requesting bureau, office or mission.